In the Specification:

Please replace the paragraph beginning on page 8 line 19 with the following amended paragraph:

At block 42, the component is re-constructed such that its structure and content will comply with the common structure of email messages. For example, if the string comprises non-ASCII characters, then these**[[s]]** characters are removed or replaced with spaces, or if the length of component string is not reasonable for the content (e.g. 200 characters for a date), then the extra characters will be removed, and so forth.

Please replace the paragraph beginning on page 9 line 12 with the following amended paragraph:

As mentioned above, a well-known vulnerability of email-related systems is the length of some of the formats, which, for example, at Base64 should be a multiple of 4, i.e. 4, 8, 12, 16, 32, 64 bytes, and so forth. According to one embodiment of the present invention, changing the format of the attachment to a valid format, not necessarily Base64, ensures that every email client that supports this format would be able to handle the data. However, there is still some chance that the "valid" attachment will not be interpreted as the invalid original. There are some solutions to this problem, e.g. recomposing the email component in such a way that the "average" email client (Outlook Express is good example) will interpret the recomposed attachment and the original attachment in the same way. In the worst case, the decomposition modifies the attachment, but then the end user gets the same data that have reached to the scanner. Indeed, it will not be the original attachment, but still a virus can be "filtered".